In the Claims

1. (Currently Amended) A method for a mobile computing device to make authentication information available to a base computing device, the method comprising:

creating authentication information, the authentication information including content data that includes data for updating a care-of address of the mobile computing device, a public key of the mobile computing device, a network address of the mobile computing device, and a digital signature, the network address having a route prefix portion and a node-selectable portion that includes a portion of a hash value of the public key of the mobile computing device ~~portion derived from the public key of the mobile computing device~~, the digital signature generated by signing with a private key of the mobile computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and

making the authentication information available to the base computing device.

2. (Previously Presented) A method as in claim 1 wherein the authentication information is made available to the base computing device by sending a message incorporating the authentication information to the base computing device.

5. (Previously Presented) A method as in claim 1, wherein the base computing device is a home agent for the mobile computing device, and wherein the network address of the mobile computing device is a home address of the mobile computing device.

6. (Previously Presented) A method as in claim 1, wherein the base computing device is a correspondent of the mobile computing device, and wherein the network address of the mobile computing device is a home address of the mobile computing device.

7. (Original) A method as in claim 1, wherein the public key and the private key together form an uncertified key pair.

8. (Currently Amended) A method as in claim 1, wherein the ~~network address of the mobile computing device includes a route prefix portion and a node-selectable portion, and the node-selectable portion includes a portion of a hash value of data including the public key of the mobile computing device.~~ node-selectable portion further comprises a hash value of a composite of the public key and a modifier.

9. (Currently Amended) A method as in claim 8, wherein the node-selectable portion ~~includes a portion of a hash value of data including the public key of the mobile computing device and a modifier selected for preventing address conflicts~~ is derived using the modifier with the public key only when

using a hash value of the public key alone as the node-selectable portion of the address creates an address that is already used by another device.

10. (Original) A method as in claim 1, wherein the authentication information further includes data for preventing a replay attack.

11. (Original) A method as in claim 10, wherein the data for preventing a replay attack are in the set: time stamp, data identifying the second computing device as an intended recipient of the authentication information.

12. (Currently Amended) A computer-readable storage medium containing instructions for performing a method for a first computing device to make authentication information available to a second computing device, the method comprising:

creating authentication information, the authentication information including content data that include data for updating a care-of address of the first computing device, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a route prefix portion and a node-selectable portion that includes a portion of a hash value of data including the public key of the mobile computing device and a modifier selected for preventing address conflicts, ~~portion derived from the public key of the first computing device,~~ the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and

making the authentication information available to the second computing device.

13. (Currently Amended) A computer-readable storage medium having stored thereon a data structure, the data structure comprising:

content data that include data for updating a care-of address of a computing device;

a public key of the computing device;

a network address of the computing device, the network address having a route prefix portion and a node-selectable portion that includes a portion of a

hash value of the public key of the mobile computing device ~~portion derived from the public key of the computing device~~; and

a digital signature, the digital signature generated by signing with a private key of the computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data.

16. (Currently Amended) A computer-readable storage medium ~~data structure~~ as in claim 13, wherein the network address of the computing device is a home address of the computing device.

17. (Currently Amended) A computer-readable storage medium ~~data structure~~ as in claim 13, wherein the node-selectable portion further comprises a hash value of a composite number derived from appending a modifier to the public key. ~~network address of the computing device includes a route prefix portion and a node-selectable portion, and the node-selectable portion includes a portion of a hash value of data including the public key of the computing device.~~

18. (Currently Amended) A computer-readable storage medium ~~data structure~~ as in claim 17, wherein the ~~node-selectable portion includes a portion of a hash value of data including the public key of the computing device and a modifier selected for preventing address conflicts.~~ modifier is used only if deriving the node-selectable portion with the public key results in a network address that is in use by another device.

19. (Currently Amended) A computer-readable storage medium ~~data structure~~ as in claim 13, wherein the data structure further includes data for preventing a replay attack.

20. (Currently Amended) A method for a second computing device to authenticate content data made available by a first computing device, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;

deriving a node-selectable portion of a second network address by taking a portion of a result of hashing [[from]] the public key of the first computing device;

validating the digital signature by using the public key of the first computing device; and

accepting the content data if the ~~derived~~ node-selectable portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated by the first computing device ~~from data in the set: the content data, a hash value of data including the content data~~.

21. (Original) A method as in claim 20, further comprising:

determining whether to accept the content data based on a time stamp in the authentication information.

22. (Original) A method as in claim 20, wherein the content data include data for updating a communications parameter for the first computing device, the method further comprising:

updating a record of a communications parameter for the first computing device.

23. (Original) A method as in claim 22, wherein the communications parameter is a care-of address of the first computing device, and wherein updating includes updating a routing table maintained by the second computing device.

24. (Currently Amended) A method as in claim 20, wherein the authentication information further includes a modifier, and wherein deriving the node-selectable portion further includes a portion of a result of hashing a composite of the modifier and the public key. ~~appending the modifier to the public key of the first computing device before deriving a portion of the second network address.~~

25. (Currently Amended) A computer-readable storage medium containing instructions for performing a method for a second computing device to authenticate content data made available by a first computing device, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, a modifier and a digital signature;

deriving a node-selectable portion of a second network address by taking a portion of a result of hashing [[from]] the public key of the first computing device;

deriving a node-selectable portion of a second network address as a hash value of a composite of the modifier and [[from]] the public key of the first computing device;

validating the digital signature by using the public key of the first computing device; and

accepting the content data if the ~~derived~~ node-selectable portion of the second network address matches a ~~corresponding~~ node-selectable portion of the first network address and if the validating shows that the digital signature was generated from a device having knowledge of a private key that corresponds to the public key of the first computing device. ~~data in the set: the content data, a hash value of data including the content data~~.